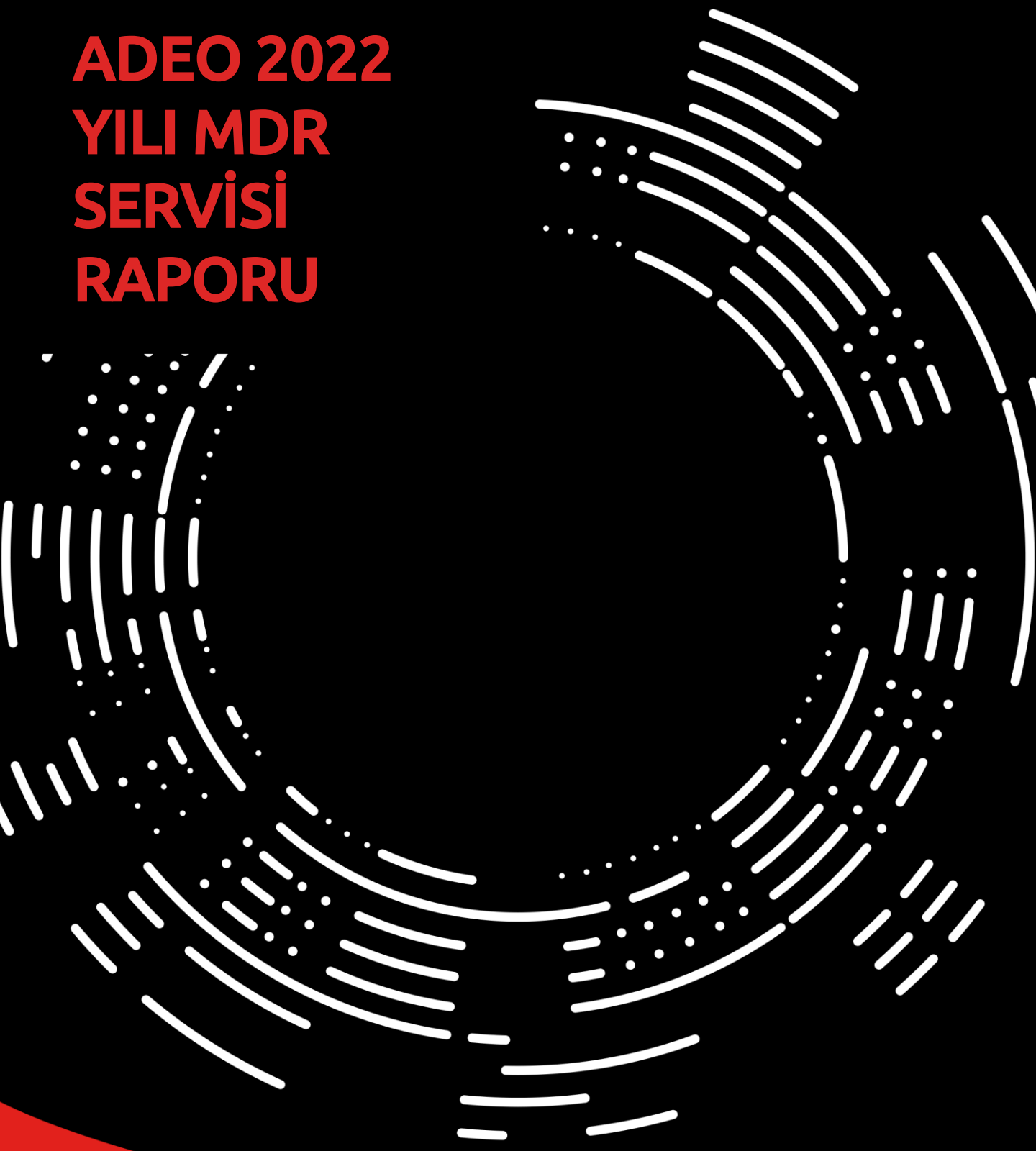
ADEO
CYBER SECURITY

ADEO 2022 YILI MDR SERVİSİ RAPORU



www.adeo.com.tr

İÇİNDEKİLER

1. ADEO MDR RAPORU HAKKINDA

Yönetilen Tespit ve Müdahale Hizmetleri (MDR), siber saldırıları mümkün olan en hızlı şekilde tespit etmek ve saldırıya hemen müdahale etmek için yürütülen çalışmalardır.

MDR, kuruluşunuz içinde tespit edilen tehditleri uzaktan izler, algılar ve yanıt verir. Bunun için hizmet sağlayıcı bir uç nokta tespit ve müdahale (EDR*) aracı kullanır ve bu sayede uç noktadaki güvenlik olaylarına ilişkin gerekli görünürlük sağlanmış olur. Gerekli görünürlük sağlandıktan sonra uç noktalardan elde edilen telemetri verileri merkez konsolda toplanır. Burada tehdit istihbarat verileri ve gelişmiş analitik yardımıyla hızlı şekilde şüpheli olayın tespiti yapılır ve müdahalesi gerçekleştirilir.

Bu araçlar MDR ekibi tarafından tespit edilen saldırıların;

- Yüksek oranda doğruluk payına sahip olmasına,
- İlgili siber olay öncesi ve sonrasında nelerin meydana geldiğinin detaylı şekilde görülebilmesine,
- Siber saldırıdan hemen sonra bu saldırıyı hızlıca önlemek için yapılacakların planlanmasına

olanak sağlamaktadır. Bu sayede hem bilinen hem de bilinmeyen siber saldırılara karşı kurumlar direnç kazanmaktadır.

MDR Analistleri gerçek zamanlı siber olay tespiti yapabilir ve tespit edilen bu siber saldırılar ile ilgili çok hızlı aksiyon alabilir.

Hızlı doğrulama ve aksiyon alma yetenekleri, gelişmiş siber saldırıların müdahalesinde çok ciddi önem taşımaktadır.

“MDR; tehdit avı, izleme ve müdahale gerçekleştirmek için teknoloji ile insan uzmanlığını birleştiren bir siber güvenlik hizmetidir.”

**EDR (Endpoint Detection and Response/Uç Nokta Tehdit Algılama ve Yanıt)*

Uç noktalarda çalışan tüm işlemleri ve bunların yapmış olduğu aktiviteleri kayıt altına alarak, atomik indikatörlerin yanı sıra davranışsal indikatörlere göre tespit ve tehdit avcılığı imkanı sağlayan ve gerektiğinde şüpheli aktivitelere ait kanıtların toplanabildiği ya da müdahale edilebildiği araçlardır.

**XDR (Extended Detection and Response/Genişletilmiş Tespit ve Müdahale)*

EDR araçlarına ek olarak başta network olmak üzere cloud, kimlik yönetimi, e-posta güvenliği gibi çeşitli kaynaklardan da kayıtlar analiz edebilen araçlardır.

ADEO MDR SERVİSİ

2022 YILINDA NELER YAPTIK?

2. 2022 İSTATİSTİKLERİ

EN YOĞUN GÜN:
7 NİSAN

7 NİSAN'DA İNCELENEN ALARM* SAYISI:
652

OLAY MÜDAHALESİ GEREKMEDEN ÇÖZÜLEN ALARM YÜZDESİ:
%99

EN ÇOK HEDEF ALINAN SEKTÖRLER VE BU SEKTÖRLERDEKİ TOPLAM VAKALAR*:

ÜRETİM
23 VAKA

ULAŞIM
7 VAKA

EN YOĞUN GEÇEN AY:
ŞUBAT

GERÇEKLEŞEN VAKA SAYISI:
5

***ALARM:**
Siber saldırıları tespit etmek için kullanılan güvenlik araçlarına düşen uyarı mesajlarına denir. Bu alarmlar kritiklik seviyelerine göre gruplandırılır.

***VAKA(INCIDENT):**
Tespit edilen gerçek bir alarmın analiz edilmesi sonucunda, derinlemesine analiz ve olay müdahalesi süreçlerinin işletilmesini gerektiren saldırgan aktiviteleridir. Çoğunlukla kısa süre içerisinde birden fazla makinede yayılım ve kalıcılık gösteren aktivitelerdir.

2022 İSTATİSTİKLERİ

"Yeni çıkan zafiyetler ADEO MDR Tehdit Avcıları tarafından 7x24x365 gün takip edilir ve ilgili kurallar yazılır."

"ADEO İstihbarat Servisi gerçek olay ve güncel saldırılardan sürekli olarak kendini geliştirmek yönünde beslenmektedir."

İlk Erişim Tekniği:
Saldırgan, çeşitli zafiyetlerden faydalanarak sisteme ilk erişimi sağlayıp, hedeflerine ulaşarak diğer taktik ve teknikleri kullanmaya başlar.

Ocak 2022'de **2000** olan Tespit Kuralı sayısı yıl sonunda **4000**'e çıkarıldı.

Ocak 2022'de **20.000** olan IOC sayısı **51.000**'e çıkarıldı.

Toplam Geliştirilen Kural Sayısı:

4000+

İçeriden ve Dışarıdan Sağlanan Tehdit İstihbaratı ile Taranan IOC Sayısı:

51K

En Çok Kullanılan İlk Erişim Tekniği*

Oltalama

%9,24

3. MDR EKİBİNİN GÜNLÜK RUTİNİ

İncelenen alarmların **%97'si ADEO MDR** ekibi tarafından müşteriye bildirilmeksizin analiz edilir ve kullanılan ürünün olgunluğuna göre gerekli **müdahale prosedürleri** uygulanır. Bu sayede müşterilerimiz güvenli bir şekilde günlük iş akışlarına odaklanabilmektedirler. Yapılan analizler ve alınan aksiyonlar raporlanır, belirli periyotlarda müşterilere iletilir.

**TRUE POSITIVE ALARM: Gerçek bir saldırı ya da istenmeyen/illegal davranış belirten alarmlardır.*

ADEO MDR ekibi günde ortalama **30** kadar yeni **tespit kuralı** yazmaktadır. Buna ek olarak yanlış pozitif (**false positive***) olarak değerlendirilen kurallar özelinde ise **sıkılaştırma/iyileştirme** çalışmaları yapılır.

**FALSE POSITIVE ALARM: Yapılan analizler sonucunda gerçek bir saldırıya işaret etmediği belirlenen ya da hatalı yazılan kurallar doğrultusunda oluşan alarmlardır.*

Alarmların **%3'ü** teyit edilir ve onay alındıktan sonra gerekli aksiyonlar uygulanır.

Tespit edilen **IP ve Domain**, **istihbarat servisleri** tarafında kontrol edilir ve ağ içerisinde iletişimde olduğu makineler incelenerek **IP bloklama** işlemi yapılır.

Zararlı yazılım tespit edilmesi sonucunda aktiviteler **tehdit avcılığı** yaklaşımıyla incelenerek zararlı yazılım yayılan makineler **izole edilir** ve **gerekli aksiyonlar** alınır.

ADEO MDR Hizmetlerimiz hakkında detaylı bilgi edinmek ve sorularınızı iletmek için bizimle iletişime geçebilirsiniz.

info@adeo.com.tr

4. YÖNETİLEN TESPİT VE MÜDAHALE VAKA YÖNETİM AŞAMALARI

GERÇEKLEŞTİRİLEN OLAY MÜDAHALE SAYISI:

52

Vaka (Incident)

Tespit edilen gerçek bir alarmın analiz edilmesi sonucunda derinlemesine analiz ve olay müdahalesi süreçlerinin işletilmesini gerektiren saldırgan aktiviteleridir.
Saldırganların sıfırıncı gün (Zero-day) zafiyetlerini sömürmeleri ya da çalışanlara ait parola/kullanıcı adı bilgilerini ele geçirmeleri gibi bazı ilk erişim teknikleri sonrasında olay müdahale prosedürleri işletilmesi gerekmektedir.
2022 yılında olay müdahalesi gerektiren ilk erişim tekniklerinin dağılımı 21. sayfada belirtilmiştir.

Vaka (Incident) Yönetim Aşamaları

Güvenlik İhlali

ADEO MDR ekibi tarafından güvenliği ihlal edilmiş makinelerin araştırılması ve tespit edilmesi ile ilgili çalışmalar yürütülmektedir.

Tespit

MDR tespit aşaması şüpheli aktivitenin sistemler üzerinde görülüp tanımlanmasını içerir.
EDR, NDR, SOAR vb. güvenlik ürünlerinden ve MDR analistlerinin yetkinliklerinden faydalanılarak tespit edilen olası acil ve kritik anomali hareketlerin **medyan tespit süresi** (Dwell Time) **3 dakika 37 saniye**'dir.

Analiz

Çeşitli güvenlik ürünleri vasıtasıyla tespit edilen şüpheli aktiviteler 7x24x365 gün ADEO MDR analistleri tarafından detaylı olarak incelenir.

Müdahale

Müdahale aşaması, analiz sonucunda zararlı olarak tespit edilen aktivitelerin durdurulması, engellenmesi ve aktivitenin kurum içerisinde yayılmaması için alınan aksiyonlardır. 2022 yılı içerisinde ADEO MDR ekibinin acil ve kritik vakalara **medyan müdahale süresi 16 dakika 27 saniye** olarak ölçülmüştür.

İyileştirme

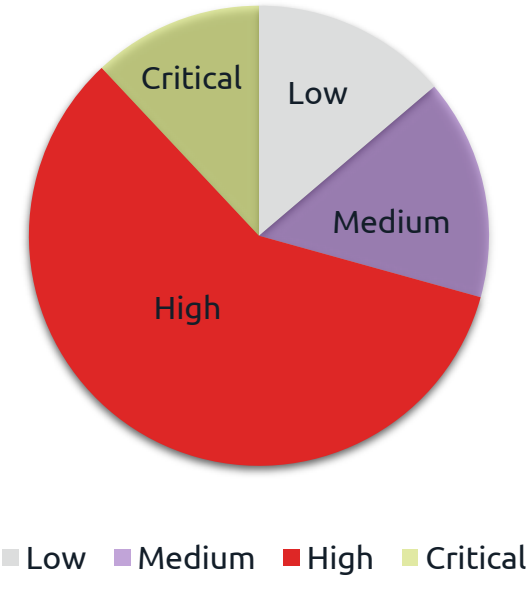
İyileştirme aşaması, tehdit oluşturan durumların ortadan kaldırılması, iyileştirilmesi ve tekrarlanmamasına yönelik önlemleri kapsamaktadır.

5. YILLIK ALARM SAYILARI VE SEVİYELERİ

ADEO'nun kural geliştirme ve iyileştirme çalışmaları sürekli olarak devam etmektedir.

Bu çalışmalar kapsamında 2022 yılı hedefi,

- Kritik ve yüksek seviyeli alarm sayılarının düşürülmesi ve
- Gerçek pozitif alarm sayılarının arttırılmasıdır.



TESPİT VE MÜDAHALE SÜRESİ

MEDYAN (MEAN) TESPİT SÜRESİ*

3dk 37s

MEDYAN (MEAN) MÜDAHALE SÜRESİ*

16dk 27s

Sadece acil ve kritik seviyedeki alarmların medyan tespit süresi **3 dakika 37 saniye**, medyan müdahale süresi ise **16 dakika 27 saniye** olarak ölçülmüştür.

**TESPİT SÜRESİ:*
Saldırının gerçekleşmesi ile saldırının MDR ekibi tarafından görülüp saldırı olarak tanımlanması arasında geçen süreye denir.

**MÜDAHALE SÜRESİ:*
Saldırının gerçekleşmesi ile, ilgili saldırının MDR Ekibi tarafından görülüp tanımlanmasının ardından gerekli aksiyonun alındığı zaman aralığına denir.

6. ALARMLARIN SEKTÖRLERE GÖRE DAĞILIMI

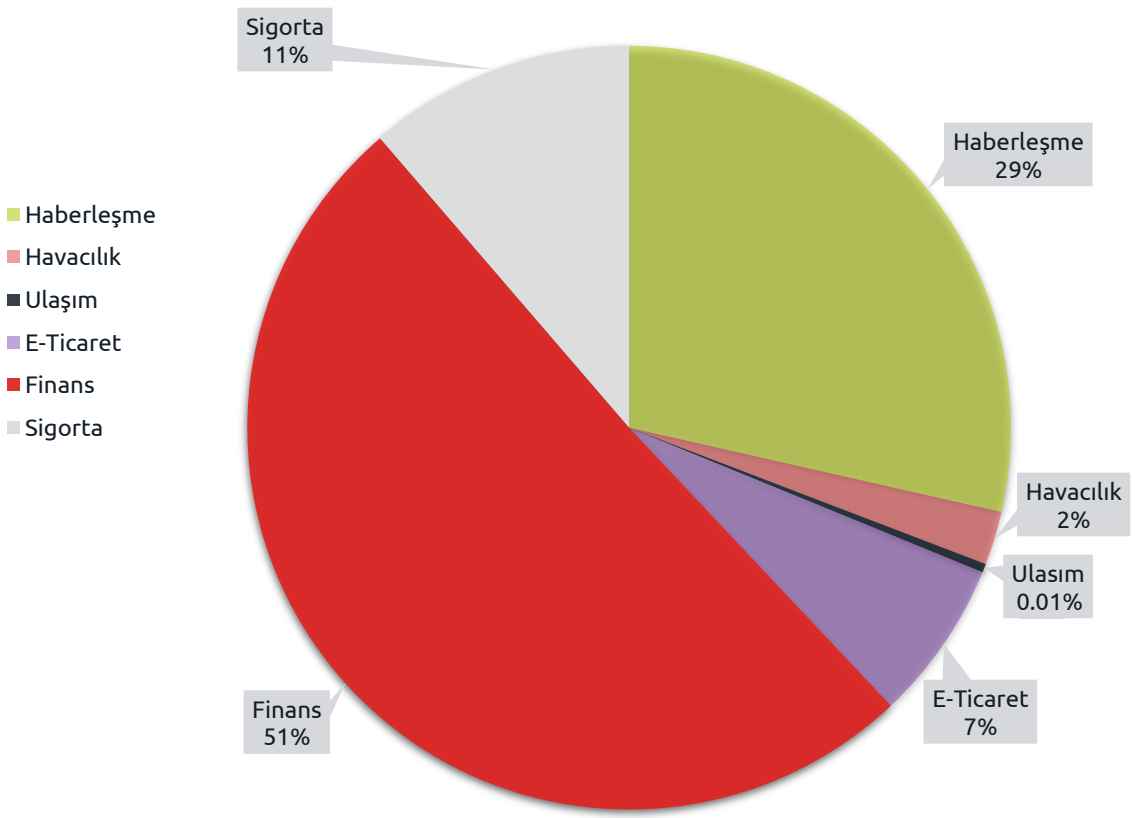
EN ÇOK ALARM GÖZLENEN SEKTÖRLER

FİNANS

Sektörün stratejik önemi çok büyüktür ve bu sebeple siber saldırı gruplarının hedefindedir.

HABERLEŞME

Çalışanların çoğunlukla sahada bulunduğu, dağıtık yapıda bir sektördür.
Saldırılara bu dağıtık yapı sebebiyle maruz kalınmıştır.



7. EN ÇOK VAKA GERÇEKLEŞEN SEKTÖRLER

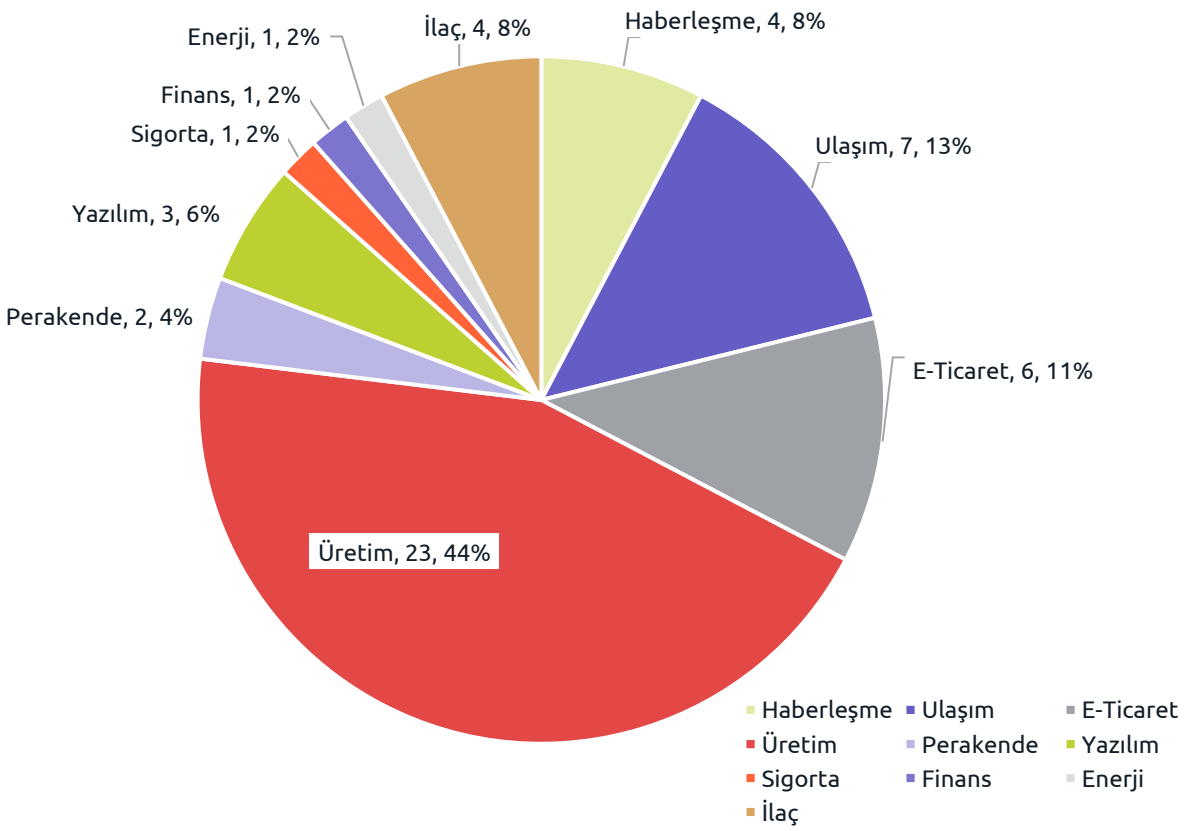
Ransomware grupları özellikle **Üretim** sektörünü hedef alıyor.

Sektör dağıtık bir yapıda ve **yönetim merkezden değil,** bölgedeki ekipler tarafından yapılıyor. Yerel ekip kontrolünde olmasından kaynaklı **farkındalık düşük** oluyor.

Bu düşük farkındalık sonucunda **görünürlük az** oluyor ve saldırı **geç tespit** ediliyor.

OT ortamlarında görünürlük düzeyinin çok düşük olması sebebiyle güvenlik standartlarının karşılanmadığı ve OT saldırılarına karşı **farkındalıkların** ya da önlemlerin **çok zayıf** olduğu görülmektedir.

Neden Üretim Sektörü?



8. 2022 YILINDA YAŞANAN ÖNEMLİ GÜVENLİK ZAFİYETLERİ & ADEO MDR SERVİSİ KURAL ÇALIŞMALARI

2022 yılında yayınlanan önemli Top 50+ güvenlik açığı hakkında **ADEO MDR** olarak **yazdığımız kurallar** ve **eklediğimiz IOC'lerin sayısı** bir sonraki sayfada tabloda gösterilmiştir. Buradan da görüleceği üzere siber olayların sayısı her geçen gün artmaktadır.

Meydana gelen siber atakların detayına indiğimizde, bu atakların tespit edilme oranı önceki saldırıların tespit edilme oranına göre düşüktür. Ürünlerin kendi tespit yeteneklerine ek olarak, yeni çıkan saldırıların tespiti için **proaktif güvenlik çözümlerine ihtiyaç** bulunmaktadır.

Bu noktada siber tehdit istahbaratı kaynaklarından yapılan düzenli araştırmalar sonucu elde edilen **tehdit göstergelerinin bloklanması** ve bu kaynaklardan elde edilen **saldırıların analiz edilip** ilgili saldırıların **tespitine dair kuralların geliştirilmesi** ve yazılan kuralların **laboratuvar ortamlarımızda test edilip ADEO kural veri tabanına eklenerek müşterilerimizin sistemleri üzerinde yaygınlaştırılması** sağlanmaktadır.

Tehdit algılama ve istihbarat analistlerimiz **yeni çıkan güvenlik açıkları** hakkında **düzenli olarak araştırmalar** yapmaktadırlar. Zafiyetler teknik olarak incelenip laboratuvar ortamlarında test edildikten sonra **tespit edilen IOC'ler** ve gözlemlenen farklı paternler özelinde **atak yüzeyinin görünürlüğünü artırmak** için **birden fazla kural seti** geliştirilmektedir.

"Yeni çıkan saldırıların tespiti için proaktif güvenlik çözümlerine ihtiyaç bulunmaktadır."

ADEO MDR Hizmetlerimiz hakkında detaylı bilgi edinmek ve sorularınızı iletmek için bizimle iletişime geçebilirsiniz.

info@adeo.com.tr

9. 2022 YILINDA YAŞANAN ÖNEMLİ GÜVENLİK ZAFİYETLERİ & SAYILARLA ADEO MDR SERVİSİ KURAL ÇALIŞMALARI

Güvenlik Açığı	Yazılan Kural Sayısı	Ürünlere Eklenen IOC Sayısı
SysJoker Backdoor	18	74
Qbot/Qakbot	25	270
CVE-2021-4034 | PwnKit: Local Privilege Escalation Vulnerability	3	97
BazarLoader	4	100
Malware Targeting Ukrainian Organizations	12	4316
ProxyNotShell Exchange Vulnerability (CVE-2022-41082, CVE-2022-41040)	14	400
B1txor20	7	114
Spring4Shell	6	250
CVE-2022-26809 Remote Procedure Call Runtime Remote Code Execution Vulnerability	3	252
CVE-2022-29072 - 7-Zip Local Privilege Escalation	3	32
BPFDoor - An Evasive Linux Backdoor	6	101
MS-MSDT 0-day RCE	6	120
Kingminer Botnet Attack	6	345
Follina Zero-Day Vulnerability (CVE 2022-30190)	3	183
LockBit 3.0 Ransomware	3	210
Domain Privilege Escalation [CVE-2022-26923]	3	229
Windows System hive/sam File Export Process	7	236
SessionManager Exchange Malware	6	194
Microsoft Teams' GIFShell Attack	6	185
Nerbian RAT Malware	6	50
X-Files Stealer – Malware	8	37
HermeticWiper and Destructive Malware Targeting Ukraine	5	63
WhisperGate: A Destructive Malware to Destroy Ukraine Computer Systems	5	70
New BianLian Ransomware	7	129
BlackByte Ransomware	7	108
Lazarus Group’s Rootkit Attack	12	840
Ryuk Ransomware	4	72
Zero-day Vulnerabilities in Microsoft Exchange Server	12	1525
BlackCat Ransomware	18	38
BumbleBee Malware	7	351
Cuba Ransomware	25	710
Black Basta Ransomware	20	125

2022 YILINDA YAŞANAN ÖNEMLİ GÜVENLİK ZAFİYETLERİ & ADEO MDR SERVİSİ KURAL ÇALIŞMALARI

İlgili güvenlik zafiyetleri ve saldırıları hakkında geliştirilen kurallar ve MDR güvenlik analistleri yetkinlikleri ile düzenli periyotlarla müşterilerimizin sistemleri üzerinde **tehdit avcılığı** gerçekleştirilmektedir. Potansiyel siber saldırıların gerçekleşmesi öncesinde ilgili zafiyetin veya saldırı göstergelerinin tespiti yapılmaktadır. Yapılan tespit sonrasında, gereken önlem ve aksiyonlar alınarak, konu özelinde kuruma bilgilendirmeler yapılır. Saldırı ile ilgili kurallar müşteri sistemlerine eklenerek, **MDR güvenlik analistleri** tarafından **7x24x365** gün boyunca **izlenmektedir**. Düzenli olarak MDR raporlarıyla müşterilerimize tespit edilen bulguların detayları paylaşılmaktadır.

Güvenlik analistleri tarafından izlenmekte olan müşteri sistemlerine kurallar eklendikten belli bir süre sonra ilgili zafiyetin istismar edilmesine dair alarmlar analistler tarafından tespit edilmektedir. Yapılan incelemeler doğrultusunda siber atakların istismarı, geliştirilen kurallar ve IOC'ler aracılığı ile engellendikten sonra analistler tarafından zafiyete sebebiyet veren **kök neden** (root cause) **araştırılmaktadır**.

Analizler sonrasında elde edilen **bulgu ve IOC** verileri ile **ADEO tehdit istihbarat kaynağı** güncellenmektedir. Saldırılara ait elde edilmiş istihbarat veri setleri düzenli olarak müşterilerimizin sistemlerine eklenmektedir. Böylelikle eklenen IOC ve istihbarat verileri ile tüm müşteri sistemleri üzerinde ilgili güvenlik açığının istismar edilmesinin önüne geçilmektedir.

"Saldırı ile ilgili kurallar müşteri sistemlerine eklenir ve müşteri sistemleri ADEO MDR güvenlik analistleri tarafından 7x24x365 gün boyunca izlenir."

10. 2022 YILININ EN SICAK GÜNDEMİ - #TOP 4

EN YOĞUN GEÇEN AY:
ŞUBAT

GERÇEKLEŞEN VAKA SAYISI:
5

EN YOĞUN GÜN:
7 NİSAN

7 NİSAN'DA İNCELENEN ALARM SAYISI:
652

"Global trendlerin kontrolü ve tehdit istihbaratlarının takip edilmesiyle, güncel zafiyetlere yönelik kurallar hızlıca eklenmektedir."

11. 2022 YILININ EN SICAK GÜNDEMİ - #1 Spring4Shell

Spring4Shell Nedir? (1)

Spring, Java için kullanılan bir framework'tür. CVE-2022-22965 kodu ile tanımlanan Spring4Shell ise Spring Framework'te bulunan ve uzaktan kod çalıştırmaya (RCE) imkan sağlayan bir güvenlik açığıdır. 2021 yılında popüler olan Log4Shell güvenlik açığına istinaden Spring4Shell ismini almıştır fakat bu güvenlik açıkları birbirleri ile ilişkili değildir.

Sıfırıncı gün (Zero-Day) güvenlik açığı daha sonradan silinen bir Twitter paylaşımı ile duyuruldu. VMware de Spring4Shell'i 31 Mart 2022 tarihinde resmi olarak açıkladı.

Spring4Shell Etkileri Nelerdir? (2)

Güvenlik açığı, JDK 9 veya üzerinde çalışan Spring MVC ve Spring WebFlux uygulamalarını etkiliyor. Webshell, genellikle siber saldırılar amacıyla bir web sunucusuna uzaktan erişilmesini sağlar. Spring4Shell güvenlik açığı için yapılan istismarların çoğu web sunucusuna zararlı bir .jsp dosyası ile webshell yüklemesi ile oluşur. Yüklenen webshell sonrasında saldırganlar uzaktan kod çalıştırabilirler.

Spring4Shell Faaliyetleri Nelerdir? (3)

- Spring4Shell güvenlik açığı yayınlandıktan **4 gün** sonra dünya çapındaki kuruluşların **%16**'sı istismar girişimlerine maruz kaldı.
- Spring4Shell güvenlik açığı yayınlandıktan sonraki ilk hafta sonunda **37.000** istismar girişimi oldu.
- Yazılım satan kurumlar (software vendors) **%28** oranla en çok etkilenen sektör oldu.
- İstismar girişimlerinden en fazla etkilenen **%20**'lik bir etki ile Avrupa kıtasıdır.

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

ADEO MDR Servisi olarak Spring4Shell zafiyetini kendi laboratuvar ortamlarımızda canlandırıp ilgili zafiyetin tespit edilebilmesi için farklı paternler kullandık. Toplam geliştirilen **6 tespit kuralı** ve çeşitli global CTI kaynaklarından **toplanan 250 zararlı IOC** tüm müşterilerimize **4 saat** içerisinde aktarılmıştır.

12. 2022 YILININ EN SICAK GÜNDEMİ - #2 ProxyNotShell

ProxyNotShell Nedir?

Microsoft, 30 Eylül 2022'de Exchange e-posta sunucularını etkileyen iki güvenlik açığı yayınladı. Bu zafiyetler, Proxyshell güvenlik açığına benzediği için ProxyNotShell olarak isimlendirildi.

Saldırganın bu güvenlik açıklarından yararlanabilmesi için kimliği doğrulanmış olması gerekir. Bu nedenle CVSSv3 skorları 8.8 olarak belirlenmiştir.

ProxyNotShell Etkileri Nelerdir?

Yayınlanan ilk güvenlik açığı CVE-2022-41040, Exchange Server'da Sunucu Tarafında İstek Sahtekarlığı (SSRF) güvenlik açığının istismar edilmesine imkan verir. ProxyNotShell'e dahil olan bir diğer güvenlik açığı olan CVE-2022-41082 ise uzaktan kod yürütmeye (RCE) olanak sağlar.

Microsoft tarafından ProxyNotShell için yayınlanan öneriler nelerdir?

Microsoft yayınladığı blog yazısında (4) Exchange Online müşterilerinin herhangi bir işlem yapmasına gerek olmadığını belirtti. Güvenlik açığı ilk açıklandığında Microsoft'un yayınladığı ilk önermeler yetersiz kaldı, sonrasında Exchange sunucuları için güncelleme yayınlandı. Microsoft yayınlanan güncellemelerin uygulanmasını önerdi.

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

ADEO MDR Servisi olarak **ProxyNotShell** zafiyetini kendi laboratuvar ortamlarımızda canlandırıp, ilgili zafiyetin tespit edilebilmesi için farklı paternler kullandık. Toplam geliştirilen **14 tespit kuralı** ve çeşitli global CTI kaynaklarından toplanan **400 zararlı IOC** tüm müşterilerimize **5 saat** içerisinde aktarılmıştır.

13. 2022 YILININ EN SICAK GÜNDEMİ - #3 Cuba Ransomware

Cuba Ransomware Grubunu Tanıyalım

Kimdir?

Cuba fidye yazılımı (ransomware) ilk olarak Aralık 2019'da gözlemlendi. Kasım 2021'de ise FBI bu fidye yazılım grubu ile ilgili resmi bir açıklama yayınlayınca bilinirliğini arttırdı. (5) Cuba fidye yazılımının, Rusça bir klavye düzeni fark edildiğinde saldırıya devam etmediği gözlemlendiği için Rusya kaynaklı bir grup olduğu düşünülüyor.

En Çok Etkilenen Ülkeler ve Sektörler?

Cuba fidye yazılımının en yüksek saldırı girişimi yaptığı ülkeler **%26**'lık oran ile **ABD**, **%21**'lik oran ile ise **Türkiye**'dir. Cuba'nın hedef aldığı sektörler araştırıldığında, **bilişim sektörünün** ilk sırada olduğu gözlemlendi. Genel olarak orta ölçekli (201-1000 çalışan) sayısına sahip şirketleri hedef aldığı bilinmektedir. Cuba fidye yazılımı grubu ProxyShell ((CVE-2021-34473, CVE-2021-34523 , CVE-2021-31207) ve ProxyLogon (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) zafiyetlerinden etkilenen kurumları hedef alarak kurumlara ilk erişimlerini sağlamışlardır. (6)

Cuba'nın 2022'de Yaptığı Bazı Saldırılar

Ağustos: Cuba Ransomware grubunun ROMCOM RAT olarak isimlendirilen ve veri yükleme gibi aktiviteleri olan yeni bir zararlı yazılım ve KerberCache isminde yeni bir araç kullandığı tespit edildi. (7)

Eylül: Cuba, Karadağ hükümetine saldırdı ve hükümet saldırıdan Rusya'yı sorumlu tutarak birtakım hassas belgelerin "dark web"de sızdırıldığını iddia etti. (8)

Ekim: Cuba ransomware grubu, Ukrayna'yı hedef alarak oltalama saldırısı düzenledi. Saldırıda oltama mailinden gelen linke tıklandığında PDF Reader'a yönlendirilip, dosya indirildiği ve ROMCOM zararlı yazılımını çalıştırdığı tespit edildi.

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

ADEO MDR Servisi olarak **Cuba** zafiyetini kendi laboratuvar ortamlarımızda canlandırıp, ilgili zafiyetin tespit edilebilmesi için farklı paternler kullandık.

Toplam **31 tespit kuralı** ve **710 IOC,** tüm müşterilerimize **6 saat** içerisinde aktarılmıştır.

14. 2022 YILININ EN SICAK GÜNDEMİ - #4 LockBit

LockBit Nedir?

LockBit fidye yazılımı, kullanıcıların bilgisayar sistemlerine erişimini engellemek ve onları fidye ödemek zorunda bırakmak amacıyla tasarlanan kötü amaçlı bir yazılımdır.

LockBit kullanımıyla gerçekleştirilen saldırılar Eylül 2019'da o günkü adıyla ".abcd virus" ile başladı. Yazılım, bugüne kadar ABD, Çin, Hindistan, Endonezya ve Ukrayna'daki kuruluşları hedef aldı. Ayrıca Avrupa genelinde birçok ülkede (Fransa, Birleşik Krallık, Almanya) saldırılar görüldü.

LockBit, 3.0 ile Tekrar Sahada

2022 Haziran ayında Lockbit fidye yazılım grubunun en son fidye yazılımı çeşidi olan LockBit 3.0'ı kullanmaya başladığı tespit edildi. Grup, bu yeni versiyonu "LockBit Black" olarak adlandırdı. LockBit 2022 Haziran ayında bir ilki başlatarak hata avcılığı (bug bounty) programını da başlatmıştır. LockBit grubundan herhangi birini tespit edebilen güvenlik araştırmacısına 1 milyon dolar teklif ettiler.

LockBit 3.0'ın 2022 Faaliyetleri

Ekim: LockBit grubu, Ekim 2022'de blog sayfalarında İngiliz otomobil bayisi olan Pendragon'u yayınladı. LockBit grubu 60 milyon dolarlık fidye talebinde bulundu fakat Pendragon fidye ödemeyi reddetti. Lockbit Pendragon verilerinin %5'ini çalabildi. Ekim ayında birkaç büyük firmaya daha saldırdılar.

Kasım: LockBit grubu, Kasım 2022'de büyük teknoloji kuruluşu olan Thales'e saldırdı. Thales fidye ödemeyi reddedince veri sızıntısına uğradı. (9)

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

ADEO MDR Servisi olarak **LockBit** zafiyetini kendi laboratuvar ortamlarımızda canlandırıp, ilgili zafiyetin tespit edilebilmesi için farklı paternler kullandık. Toplam **31 tespit kuralı** ve **210 IOC** tüm müşterilerimize **3 saat** içerisinde aktarılmıştır.

2022 YILININ EN SICAK GÜNDEMİ - TOP 4

Kaynakça

1 – https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

2 – https://kb.vmware.com/s/article/88203

3 - https://blog.checkpoint.com/2022/04/05/16-of-organizations-worldwide-impacted-by-spring4shell-zero-day-vulnerability-exploitation-attempts-since-outbreak/

4 - https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

5- https://www.cisa.gov/uscert/ncas/alerts/aa22-335a

6 - https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-cuba

7 - https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

8 - https://www.reuters.com/world/europe/montenegro-blames-criminal-gang-cyber-attacks-government-2022-08-31/

9 - https://www.avertium.com/resources/threat-reports/an-update-on-lockbit-3.0

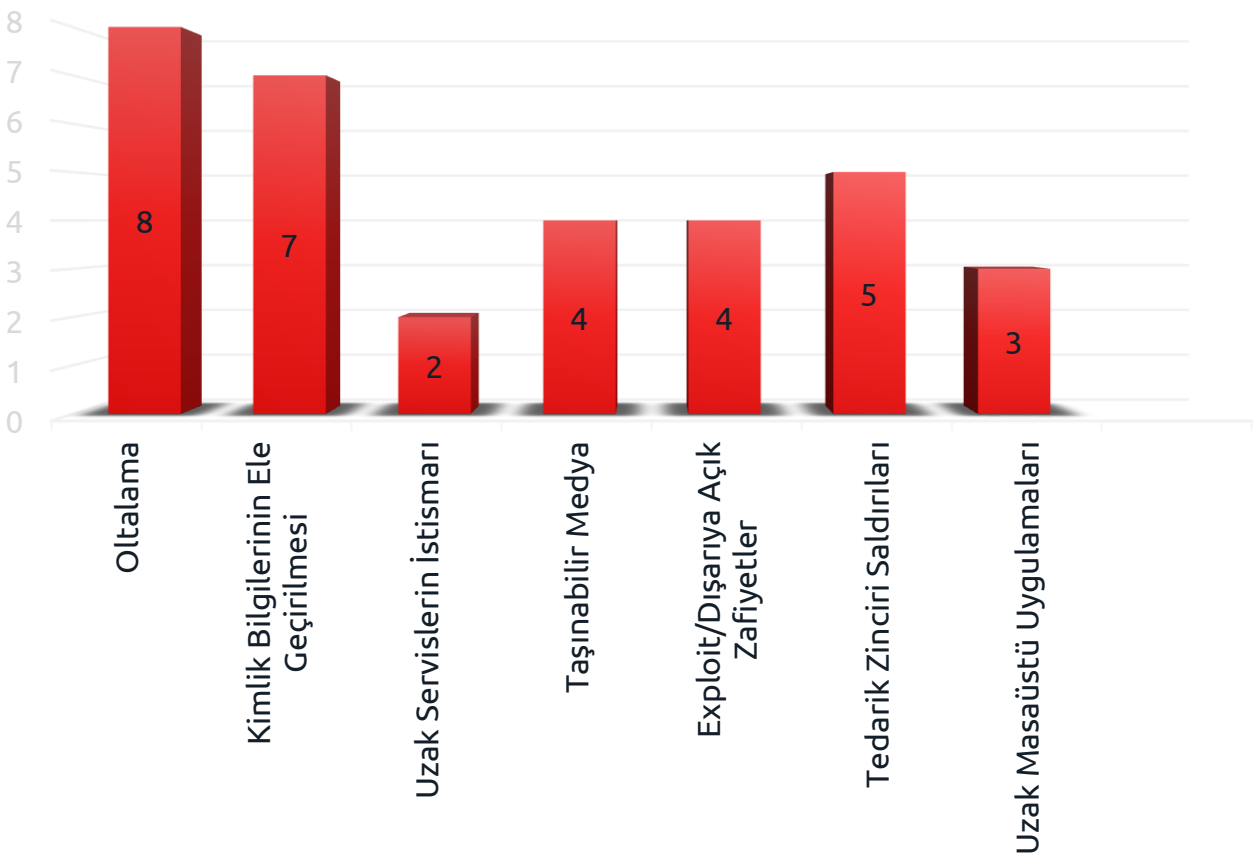
15. EN ÇOK KULLANILAN İLK ERİŞİM TEKNİKLERİ

Bir saldırganın ortamda yer edinebilmesi ilk erişim (initial access) ile başlar.

Güvenliği ihlal edilmiş hesapların kimlik bilgileri, çeşitli tekniklerle ele geçirilerek ağ içindeki sistemlerde farklı kaynaklara uygulanan erişim denetimlerini atlamak için kullanılabilir.

Saldırgan ilk erişimin ardından hedeflere ulaşmak için diğer taktik ve tekniklere geçiş yapabilir. Dolayısıyla ilk erişimin engellenmesi sistemin güvenliği açısından önem arz etmektedir.

"İlk erişimin engellenmesi sistemin güvenliği açısından büyük önem arz etmektedir."



ADEO MDR SERVİSİ

TAKTİKLER*, TEKNİKLER & TESPİT KURALLARIMIZ

**TAKTİK:*
Saldırgan tarafından gerçekleştirilen aktivitelerin amacını belirtir. Saldırının aşamasını belirlemede büyük önem arz etmektedir.

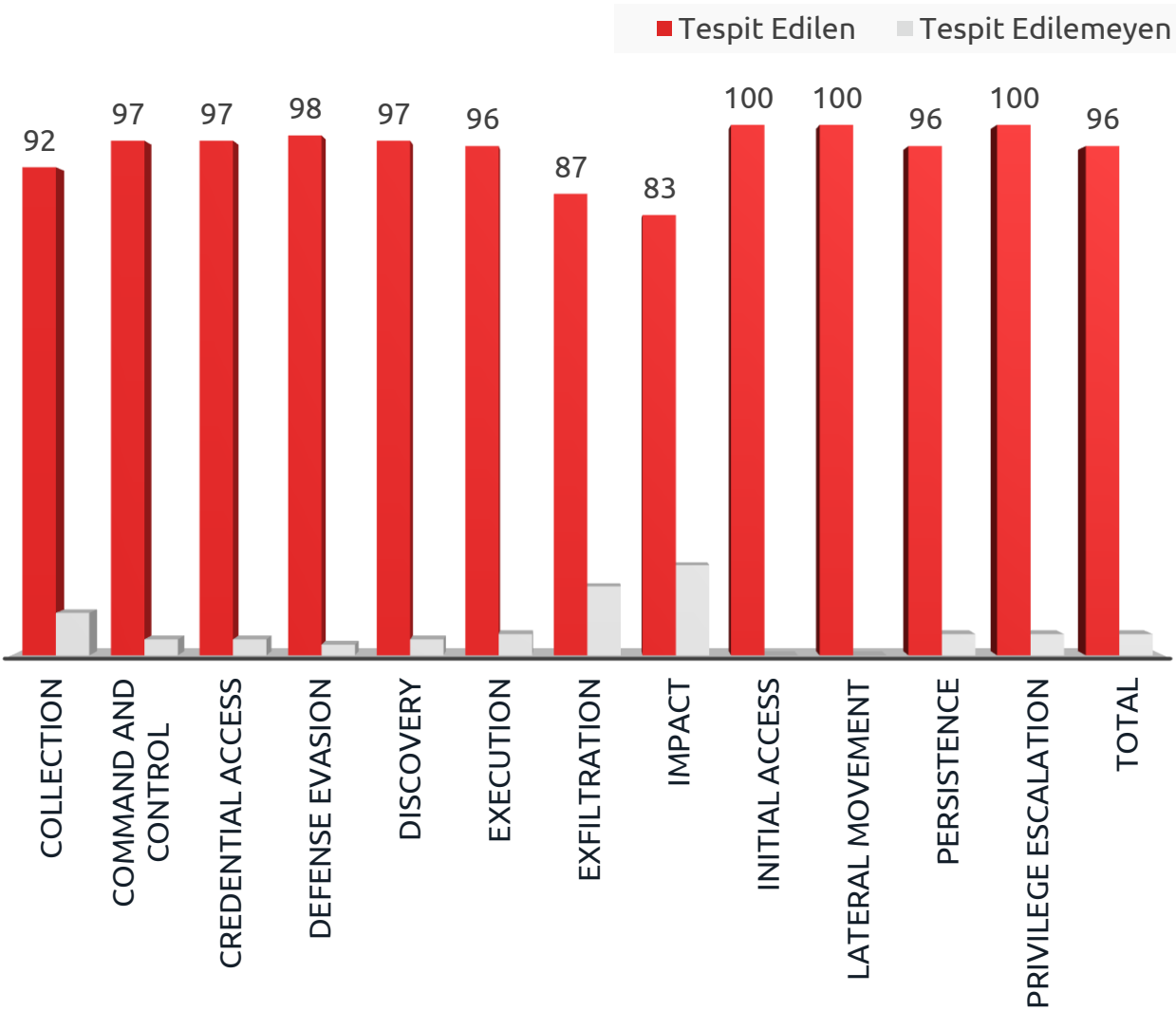
**TEKNİK:*
Saldırganların bu taktikleri gerçekleştirmek için kullandığı araçlar, yöntemler veya süreçlerdir

16. SALDIRI TESPİT KURALLARIMIZ

ADEO MDR Servisi olarak MITRE ATT&CK® Framework'de bulunan tüm taktikleri geliştirmiş olduğumuz özel algılama kuralları, tehdit istihbaratı platformlarından topladığımız IoC'ler ve güçlü lider ürün portföyümüz aracılığı ile tespit edebilmekteyiz.

MDR Servisi, gerçekleştirdiği güvenlik testlerinin sonucu olarak, EDR aracılığı ile **465 teknikten %96'sının tespit edilebildiği** raporlanmıştır. Tespit edilmeyen **18** teknikten ise sadece **5 tanesinin EDR ile tespit edilebilir** olduğu gözlemlenmiştir.

"MDR Servisi, gerçekleştirdiği güvenlik testlerinin sonucu olarak, EDR aracılığı ile 465 teknikten %97'sinin tespit edilebildiği raporlanmıştır. "



17. TAKTİKLER

1. VERİ TOPLAMA (COLLECTION)

Saldırgan, amacına uygun verileri toplamaya çalışır.

Bu taktik, saldırganın amacına hizmet eden verileri toplamak için kullandığı tekniklerden oluşur.

Genellikle hedef alınan kaynaklar arasında çeşitli sürücü tipleri, tarayıcılar, ses ve video dosyaları ve e-postalar bulunur.

Ekran görüntüsü alma, klavye girişi takip etme yaygın yöntemler arasındadır.

Veri Toplama (Collection) taktiği kullanılarak yapılan saldırıların **%92'si ADEO MDR Servisi** tarafından tespit edilebilmektedir.

Bu ve benzeri saldırıların tespiti için **EDR teknolojisine ek olarak,** veri kaybı önleme sistemlerinin uygulanması önerilir. Saldırı riski, etkisi ve derecesinin azaltılması gibi kontrolleri planlamak ve politikaların sürekliliğinin sağlanması gibi çalışmalar için ek veri sızıntısı engelleme sistemi olan **DLP** teknolojisi kullanılması tavsiye edilir.

Sıkıştırılmış veya şifrelenmiş dosyaların sızdırılma teşebbüslerini engellemek ve kullanıcı davranış analizlerini **(UBA)** yapabilmek için **XDR, NDR, Firewall, DLP** vb. teknolojilerin kullanılması tavsiye edilir.

Kullanıcı farkındalığının artırılması için düzenli periyotlarda **farkındalık eğitimleri**nin organize edilmesi önem arz etmektedir.

Kullanılan sistem imajlarının ve **yazılımlarının güncel tutulması** tavsiye edilir.

Exchange ortamında, yöneticilerin kötü amaçlı olabilecek otomatik iletme, indirme ve açma gibi etkinliklerini engellemek için **Exchange** kurallarının sıkılaştırılması gerekmektedir.
Dışarıdan erişime açık e-posta sunucuları için **çok faktörlü kimlik doğrulamasının (MFA)** kullanılması saldırıları büyük oranda azaltacaktır.

17. TAKTİKLER

2. KOMUTA VE KONTROL (COMMAND AND CONTROL)

Saldırgan kontrolü ele geçirmek için güvenliği ihlal edilmiş sistemlerle iletişim kurmayı dener. Bunu yaparken tespit edilmekten kaçınmak için genellikle normal, beklenen trafiği taklit etmeye çalışır.

Komuta ve Kontrol (**C&C**), saldırganların kendi kontrolleri altındaki sistemlerle bir hedef network aracılığı ile iletişim kurduğu tekniklerden oluşur.

Saldırganın komuta ve kontrol taktiğini oluşturmasının, saldırı altındaki network'ün yapısına ve savunmasına bağlı olarak çeşitlilik gösteren birçok yolu vardır.

Komuta ve Kontrol (Command and Control) taktiği kullanılarak yapılan saldırıların **%97'si ADEO MDR Servisi** tarafından tespit edilebilmektedir.

Bilinen **kötü veya şüpheli etki alanlarına (Domain)** giden/gelen **web trafiğinin izlenmesi** gerekmektedir**.**

DNS isteklerinin; bilinmeyen, güvenilmeyen veya bilinen kötü etki alanlarına ve kaynaklara **firewall üzerinden filtrelenmesi** tavsiye edilir.

Bu ve benzeri saldırıların tespiti için EDR'a **ek Firewall, NDR, IDS/IPS;** kullanıcı davranışı analizleri için **UBA** tabanlı ürünlerin kullanılması tavsiye edilir.

Network'te oluşan **trafiğin izlenmesi** ve içeriden dışarıya giden ve dışarıdan gelen IP'lerin **istihbarat servisleriyle sürekli olarak kontrol edilmesi** gerekmektedir.

Sisteme yüklenebilen uygulamaların onay mekanizmasından geçmesi ve izin verilen uygulamalar listesinde **(White List)** olması zorunlu kılınmalıdır. Bilgisayar sisteminiz herhangi bir uygulamanın çalıştırılmasına veya yüklenmesine izin vermemelidir. Bilinmeyen kaynaklardan uygulamaların **yüklenmesini engelleyerek**, C2 kanalları oluşturmak için kullanılan **kötü amaçlı yazılımların sisteminize yüklenmesini önleyebilirsiniz.**

17. TAKTİKLER

3. KİMLİK BİLGİLERİ ERİŞİMİ (CREDENTIAL ACCESS)

Saldırgan bu taktik ile hesap adlarını ve parolalarını çalmayı dener.

Kimlik bilgilerini almak için kullanılan yaygın teknikler arasında keylogging ve kimlik bilgisi dökümü (**Credential Dumping**) bulunur.

Meşru kimlik bilgilerinin kullanılması, saldırganların sisteme erişmesini sağlayabilir, tespit edilmelerini zorlaştırabilir ve hedeflerine kolay ulaşmalarına yardımcı olacak daha fazla hesap oluşturmalarına olanak sağlar.

Kimlik Bilgileri Erişimi (Credential Access) taktiği kullanılarak yapılan saldırıların **%97'si ADEO MDR Servisi** tarafından tespit edilebilmektedir.

WAF, kuruluşlar tarafından web sistemlerini sıfırıncı gün istismarlarına, uzaktan komut çalıştırmaya, diğer bilinen ve bilinmeyen tehdit ve güvenlik açıklarına karşı koruma sağlayan yaygın **bir güvenlik kontrolü** olup, **kurum içinde konumlandırılması** önem arz etmektedir .

Parolaların farklı platformlarda kullanılmaması, parolanın **en fazla 1 veya 3 aylık periyotlarda değiştirilmesi** ve özel karakter barındırmasına dikkat edilmesi gerekmektedir. **Gereksiz/fazla yetkilendirmeden kaçınılması**, personel işten çıktıktan sonra mevcut hesaplarının kapatılması önem arz etmektedir. **Dosya paylaşımları** yalnızca gerekli kullanıcılara erişimi olan **belirli dizinler ile sınırlandırılmalıdır.**

Kritik kaynaklara erişim izinlerine sahip kullanıcıların hesaplarının güvenli bir şekilde yönetilmesi için **Ayrıcalıklı Erişim Yönetimi – Privileged Access Management (PAM)** ürünlerinin kurum içinde konumlandırılması tavsiye edilir.

Başta VPN ve E-posta erişimleri olmak üzere, mümkün olan bütün girişlerde **MFA aktif edilmesi** önem arz etmektedir.

VLAN kullanılarak departmanların birbirinden izole edilmesi ile olası tehlikelerin en aza indirilmesi konusu önem arz etmektedir. Başta Domain Controller sunucuları olmak üzere **Kimlik bilgilerinin barındırıldığı** uygulamaların **güvenlik güncellemelerinin** düzenli periyotlarda yapılması tavsiye edilir.

17. TAKTİKLER

4. SAVUNMAYI ATLATMA (DEFENSE EVASION)

Saldırgan tespit edilmekten kaçınmaya çalışır.

Savunmayı Atlatma, saldırganların yarattıkları tehlike boyunca tespit edilmekten kaçınmak için kullandıkları tekniklerden oluşur.

Savunmayı Atlatma için kullanılan teknikler arasında güvenlik yazılımının kaldırılması/devre dışı bırakılması veya veri ve komut dosyalarının gizlenmesi/şifrelenmesi yer alır.

Saldırganlar ayrıca kötü amaçlı yazılımlarını gizlemek ve maskelemek için güvenilir süreçleri kötüye kullanır.

Savunmayı Atlatma (Defense Evasion) taktiği kullanılarak yapılan saldırıların **%98'i ADEO MDR Servisi** tarafından tespit edilebilmektedir.

PowerShell ve **Command Prompt** komut satırı uygulamaları aracılığı ile yapılan aktivitelerin analiz edilebilmesi için ilgili uygulamaların **log**larının merkezi bir noktada **kaydedilmesi/arşivlenmesi** önerilir.
Hizmet engelleme saldırılarından (**DoS / DDoS**) korunmak ve atak türlerini minimize etmek için **Load Balance** (Yük Dengeleme), **DDoS Protection**, ürünlerinin kurum içinde konumlandırılması tavsiye edilir.

Kullanıcı **ayrıcalıklarının sınırlandırılması** önerilir.
Yalnızca yetkili kullanıcılar hizmet değişiklikleri yapabilecek şekilde sınırlanmalıdır.
Dosya indirme dizinleri ve geçici dosya (Temporary Files) dizinleri gibi kullanıcı dizinlerinden **yürütmenin engellenmesi** önerilir.

Saldırganlar, kötü amaçlı kodu gizlemek için derlenmiş **HTML dosyalarını (.chm)** kötüye kullanabilir. CHM dosyaları genellikle Microsoft HTML yardım sisteminin bir parçası olarak dağıtılır. CHM dosyaları **VBA, JScript, Java ve ActiveX** gibi çeşitli içeriklerin sıkıştırılmış derlemeleridir. **Application whitelist yazılımları** ile bu tarz yaygın kullanılmayan **script uzantılarının** çalıştırılması **engellenebilir** ya da **tespit** edilebilir.

Kurum içinde **ihtiyaç duyulmayan uygulamaların** güvenlik açığı verebilecek özelliklerinin **devre dışı bırakılması/kaldırılması** önerilir.
E-posta yolu ile yapılan **oltalama saldırılarının** önlenmesi için **Sandbox** türevi teknolojilerin ve **Email Security Gateway** ürünlerinin konumlandırılması, kullanılan **uygulama envanterlerinin** düzenli periyotlarda **güvenlik güncelleştirmelerinin yapılması** önem arz etmektedir.

17. TAKTİKLER

5. KEŞİF (DISCOVERY)

Saldırgan hedefini tanımaya, keşfetmeye çalışır.

Keşif, saldırganın sistem ve dahili network hakkında bilgi edinmek için kullanabileceği tekniklerden oluşur. Bu teknikler, saldırganın nasıl hareket edeceğine karar vermeden önce çevreyi gözlemlemesine ve planına yön vermesine yardımcı olur.

Bu teknikler saldırgana ayrıca neyi kontrol edebileceği ve giriş noktalarının çevresinde neler olabileceği konusunda fikir verir, fayda sağlar.

Keşif (Discovery) taktiği kullanılarak yapılan saldırıların **%97'si ADEO MDR Servisi** tarafından tespit edilebilmektedir.

Kurumlarda var olan ortam (**Active Directory, Firewall, Network Segmentasyon** ve varsa diğer güvenlik cihazlarının yardımı ile) ihtiyaca uygun şekilde sıkılaştırılarak, **atak yüzeyi daraltılmalıdır**. Ortamlar üzerinde çalışan **Audit** ve **Log seviyelerinin** sıkılaştırılması ve olgunlaştırılması tavsiye edilir.

Keşif ve olası sömürü riskini önlemek için varlık envanterlerinin belirli periyotlarda incelenmesi, **gereksiz bağlantı noktalarının, hizmetlerin ve servislerin kapalı** olduğundan emin olunması gerekmektedir.

Uzaktan hizmet taramalarını algılamak ve önlemek için **IPS/IDS teknolojilerinin** kullanılması tavsiye edilir.

Birçok önemli bilgi, Windows Yönetim Araçları ve PowerShell gibi Windows sistem yönetim araçları aracılığıyla da edinilebilir. Sistem ve ağ bilgilerini toplamak için gerçekleştirilebilecek bu tarz eylemleri tespit edebilmek için **Windows event logları** yapılandırılmalı ve merkezi olarak toplanmalıdır.

Varlık envanterinde olan uygulamaların **güvenlik güncelleştirmeleri** düzenli periyotlarda kontrol edilmelidir.

Kullanıcı hesap yönetimi sağlanmalı, **minimum ayrıcalık ilkesi** uygulanmalıdır.

17. TAKTİKLER

6. YÜRÜTME (EXECUTION)

Yürütme, yerel veya uzak bir sistemde saldırganın kontrolündeki kodun çalıştırılmasını sağlayan tekniklerden oluşur.

Kötü amaçlı kod çalıştıran teknikler, bir network'ü keşfetmek veya veri çalmak gibi daha geniş hedeflere ulaşmak için genellikle diğer tüm taktiklerdeki tekniklerle eşleştirilir. Örneğin bir saldırgan, uzaktan sistem keşfi yapan bir Powershell betiğini çalıştırmak için bir uzaktan erişim aracı kullanabilir.

Yürütme (Execution) taktiği kullanılarak yapılan saldırıların **%96'sı ADEO MDR Servisi** tarafından tespit edilebilmektedir.

Kullanıcı, kötü amaçlı bir dosyayı veya bağlantıyı açarak kötü amaçlı kod yürütmek için sosyal mühendislik saldırısına maruz kalabilir. Bu tür saldırıları önlemek için son kullanıcı tarafındaki e-posta ya da internet tarayıcı **uygulamalarının denetiminin ve güncellemesinin düzenli periyotlarda yapılması gerekmektedir.**

Saldırganların **RCE zafiyetinden yararlanmalarını** engellemek ya da tespit etmek için **NGFW** veya **NDR** ürünleri ile ağ trafiği üzerindeki görünürlük artırılmalıdır.

Kurumlarda var olan ortam **(Active Directory, Firewall, Network Segmentasyon ve varsa diğer güvenlik cihazlarının yardımıyla)** ihtiyaca uygun şekilde sıkılaştırılarak, **atak yüzeyi daraltılmalıdır**. Ortamlar üzerinde çalışan **Audit** ve **Log seviyelerinin** sıkılaştırılması, olgunlaştırılması ve **SIEM** teknolojilerinin kullanılması tavsiye edilir.

Dışarıya açık sunucularda bulunabilecek bir **RCE zafiyeti** saldırganın kolaylıkla kurum ağına girmesini sağlayacaktır. **Zero Trust** güvenlik stratejisi ile dışarıya açık sunuculardan içeriye ya da diğer sunuculara **yapılan erişimler, ağ erişim kontrolü (NAC) araçları** ile **sınırlandırılmalı** ve **takip edilmelidir.**

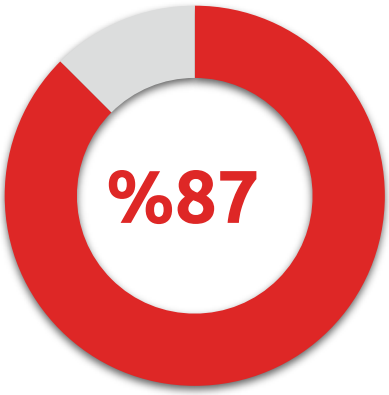
17. TAKTİKLER

7. VERİ KAÇIRMA (EXFILTRATION)

Veri Kaçırma, saldırganların ağınızdan veri çalmak için kullandığı tekniklerden oluşur. Saldırganlar verileri topladıklarında tespit edilmekten kaçınmak için onları sıkıştırma ve şifrelemeyi içerebilecek biçimde paketler.

Hedef bir ağdan veri elde etme teknikleri, tipik olarak, verinin kendi komuta ve kontrol kanalı veya alternatif bir kanal üzerinden aktarılmasını içerir. Ayrıca aktarıma boyut sınırları da koyulabilir.

Veri Kaçırma (Exfiltration) taktiği kullanılarak yapılan saldırıların **%87'si ADEO MDR Servisi** tarafından tespit edilebilmektedir.



Verilerin ağdan ayrılabilmesi için tasarlanmış bir çıkış noktasından geçmesi gerektiğinden, tipik olarak C2 algılaması için yararlı olan imza tabanlı virüsten koruma özelliklerine sahip, **yeni nesil bir güvenlik duvarı (NGFW)** veya trafik protokollerini görebilen ağa izinsiz giriş önleme sistemi **(IPS) sızıntıyı tespit etmeye ve önlemeye yardımcı olabilir**.

DLP, kullanıcı tarafından hassas verilere yetkisiz olarak erişimi ve bu verilerin kullanımını izler. Verilerin dışarı çıkmasını önlediği için kullanılması tavsiye edilir.

Saldırganlar, **USB üzerinden** zararlı kodu çalıştırarak, ağ üzerinden yayılırlar. Bazı durumlarda bir kullanıcı tarafından tanıtılan bir **USB aygıtı aracılığıyla veri kaçırma gerçekleşebilir**. USB aygıtı, son veri kaçırma noktası olarak veya başka şekilde bağlantısız sistemler arasında geçiş yapmak için kullanılabilir. Bunun önüne geçebilmek için **farkındalığın düşük olduğu yerlerde usb portlarının devre dışı bırakılması önerilir.**

Saldırgan, verileri tek parça göndermek yerine **dosyaları parçalayarak gönderebilir.** Bu şekilde minimum yükleme boyutunu aşmadan verinin iletimini sağlar. Saldırıyı önlemek için **network trafiğinin sürekli olarak izlenmesi** önerilir.

17. TAKTİKLER

8. ETKİ (IMPACT)

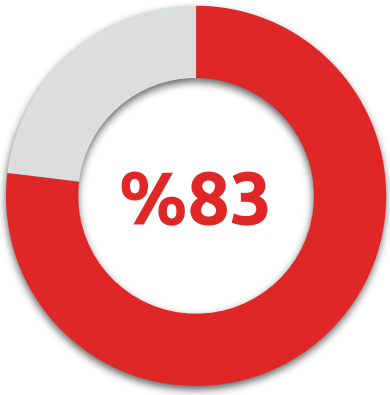
Saldırgan, sistemlerinizi ve verilerinizi manipüle etmeyi, kesmeyi veya yok etmeyi dener.

Etki, saldırganların iş ve operasyonel süreçleri manipüle ederek kullanılabilirliği bozmak ve bütünlüğü tehlikeye atmak için kullandığı tekniklerden oluşur.

Etki için kullanılan teknikler verileri yok etme veya bozmayı içerebilir. Bazı durumlarda iş süreçleri iyi görünebilir, sorunsuz durur ancak saldırganın hedeflerine fayda sağlayacak şekilde değiştirilmiş olabilir.

Bu teknikler saldırganlar tarafından nihai hedeflerine ulaşmak veya bir gizlilik ihlalini örtmek için kullanılabilir.

Etki (Impact) taktiği kullanılarak yapılan saldırıların **%83'ü ADEO MDR Servisi** tarafından tespit edilebilmektedir.



Fidye yazılımı, sistem ve ağ kaynaklarına **erişimi kesmek** için hedef sistemlerdeki veya bir ağda bulunan çok sayıda sistemdeki verileri şifreleyebilir. Saldırıları önlemek için **felaket senaryoları hazırlanarak yedekler alınması** ve bu yedeklerin saldırganlar tarafından erişilmez hale getirilmesi önerilmektedir.

DDoS saldırısında; saldırıya uğrayan kaynağın, birden çok makineden gelen isteğe maruz kalmasıyla kapasiteyi aşarak yanıt vermemesi ile hizmet engelleme saldırısı başarıyla sonuçlanır. **DDOS önlemek için** trafiği filtreleyerek **İçerik Dağıtım Ağları (CDN)** veya **DoS** azaltma konusunda uzmanlaşmış sağlayıcılar tarafından sağlanan **DDoS önleme hizmeti alınması** önerilmektedir.

Veri Manipülasyonu: Saldırganlar, farklı sonuçlar ile faaliyetlerini gizleyerek verileri ekleyebilir, silebilir. Bu şekilde rakibinin verilerini manipüle ederek bir iş sürecini, organizasyonel anlayışı veya karar vermeyi etkilemeye çalışabilir. Oluşabilecek maddi kayıpları önlemek için **veriyi şifreleme, saklama yöntemi** ve **DLP** çözümlerinin kullanılması önerilir.

Man in the middle saldırısı ağda iki bağlantı arasındaki iletişimin dinlenmesi ile çeşitli verilerin ele geçirilmesi veya iletişimi dinleyip yanıltıcı bir iletişim oluşturarak verinin manipüle edilmesi şeklinde gerçekleşen bir saldırı yöntemidir. **MitM** saldırı türlerini önlemek için **SSH, IPSec** protokollerinin, **HTTPS** destekli sitelerin kullanılması, public ortamlarda paylaşılan şifresiz **WIFI** ağlarına bağlanmamaya dikkat edilmesi önemlidir.

17. TAKTİKLER

9. KALICILIK (PERSISTENCE)

Kalıcılık, saldırganın sistem erişiminin sürekliliğini sağlamayı hedefleyen tekniklerden oluşur.

Kalıcılık için kullanılan teknikler, meşru kodu değiştirme/ele geçirme veya başlangıç kodu ekleme gibi sistemlerde yerlerini korumalarına izin veren tüm erişim, eylem ve yapılandırma değişikliklerini içerir.

Kalıcılık (Persistence) taktiği kullanılarak yapılan saldırıların **%96'sı ADEO MDR Servisi** tarafından tespit edilebilmektedir.

NDR, tüm bağlantı ve protokollerde size şeffaflık sağlar. Bağlantıları, akışları, paketleri ve meta verileri gerçek zamanlı olarak analiz etmek için trafiği derinlemesine tarar ve geriye dönük analiz yapar. **Algılanan bir tehdidin çözüm süresini en aza indirmek** için entegre bir **network algılama ve müdahale** çözümü kullanılması tavsiye edilir.

Önleme: Haftalık olarak ağda olan tüm cihazlar için **zararlı yazılım taraması** yaptırılması önem arz etmektedir. Ayrıca belirli aralıklarla **güvenlik ihlali analiz ve değerlendirme (Compromise Assessment)** çalışması yapılmalıdır.

Saldırganlar çeşitli zafiyetler barındıran varlıklarda **uzaktan komut çalıştırarak,** sistemlerde **sistem kapatma/yeniden başlatma işlemi** yaparak verilerin bozulmasına, e-ticaret ve hastane gibi ortam ve yerlerde maddi zararlara ve can kayıplarına sebebiyet verebilir. Bu ve benzeri atak türlerinin önlenebilmesi için **Extended Detection and Response (XDR), Firewall, Backup (yedekleme)** teknolojilerinin kullanılması tavsiye edilir.

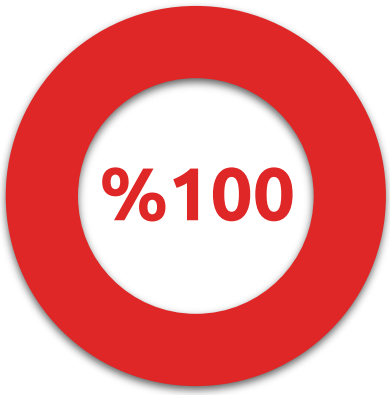
Korsan/Cracklenmiş program, oyun, işletim sistemi gibi yüklemeler sisteminizi ciddi saldırıların hedefi yapabilir. Kurumların fidye, veri ihlali, arka kapı gibi saldırılara maruz bırakılmasına yol açabilir. Bu ve benzeri saldırılar genellikle **kullanıcı farkındalığının az olmasından** kaynaklanır. Bu sebeple çalışanlara düzenli periyotlarda **temel güvenlik eğitimlerinin verilmesi tavsiye edilir.**

17. TAKTİKLER

10. YETKİ YÜKSELTME (PRIVILEGE ESCALATION)

Yetki Yükseltme, saldırganın bir sistem veya ağ üzerinde daha üst düzey izinler elde etmek için kullandığı tekniklerden oluşur. Saldırganlar genellikle ayrıcalıksız erişime sahip bir ağa girip keşif yapabilir ancak hedeflerini takip edebilmek için artırılmış izinlere ihtiyaç duyar. Yaygın yaklaşımlar, sistem zayıflıklarından, yanlış yapılandırmalardan ve güvenlik açıklarından yararlanmaktır. Yükseltilmiş erişim örnekleri şunları içerir;

- Sistem/ Kök seviyesi (Root Level)
- Domain yöneticisi (Domain Administrator),Yerel yönetici (Local Administrator)
- Yönetici benzeri erişime sahip kullanıcı hesabı (admin-like access),
- Belirli bir sisteme erişimi olan veya belirli bir işlevi yerine getiren kullanıcı hesapları



Bir saldırganın varlığını sürdürmesine izin veren işletim sistemi özellikleri yükseltilmiş bir bağlamda yürütülebildiğinden, bu teknikler genellikle "**Persistence (Kalıcılık)"** taktiği ile örtüşür.

Yetki Yükseltme (Privilege Escalation) taktiği kullanılarak yapılan saldırıların **%100'ü ADEO MDR Servisi** tarafından tespit edilebilmektedir.

Active Directory (AD) veya LDAP gibi dizin sunucularından gelen logların yapılandırılması gerekmektedir. Kullanıcı hak yükseltme veya yeni kullanıcı oluşturma olaylarının takip edilmesi gerekmektedir. Yetkili kullanıcı hesap adlarının, yetkilerinin bir **listesinin oluşturulması** gerekmektedir. **Kimlik tabanlı güvenlik (Identity-based Security)** ürünleri kullanılarak yetki yükseltme saldırıları ya da yetkili kullanıcılara yönelik saldırılar tespit edilebilir.

Ayrıcalıklı erişim haklarının uygun aralıklarla (ayda en az 1 kez) gözden geçirilmesi ve **ayrıcalıklı izinler** atamasının **düzenli olarak gözden geçirilmesi gerekmektedir**. Dosyalara ve veri tabanlarına olan (yerel sistem erişimi dahil) tüm **ayrıcalıklı kullanım erişimlerinin izlenmesi gerekmektedir**. Kritik ayrıcalıklı kullanıcı değişikliklerinin alarm mekanizmalarının Mail-SMS oluşturularak ilgili **BT yöneticileri ile anlık olarak paylaşılması gerekmektedir.**

Kullanıcıların **kötü amaçlı** dosyaları yürütmek için yerleştirebileceği yerleri azaltmak adına **dizin erişim denetiminin ayarlandığından emin olun.** Tüm yürütülebilir dosyalarda **yazma korumalı** dizinlere yerleştirilmesi tavsiye edilir.

Güvenlik açıklarını saldırganlar bu zafiyetlerden faydalanmadan tespit etmek önem taşımaktadır. **Güvenlik açığı tarama araçları** ile yapılan etkili bir tarama işlemi; sistemdeki **yanlış yapılanmaları, zayıf parolaları ve Web Sunucusu Güvenliği'ndeki zayıflıkları** ortaya çıkarır.
Etkili güvenlik açığı taraması ile kuruluşlar, tehdit vektörlerini uzak tutmak için ek güvenlik katmanlarını **güncelleyebilir, yamalayabilir veya dağıtabilir.**

17. TAKTİKLER

11. İLK ERİŞİM (INITIAL ACCESS)

İlk Erişim, saldırganın hedef ağ içerisinde birincil dayanağını elde etmesine yarayan çeşitli giriş vektörlerinin kullanıldığı tekniklerden oluşur.

Bir erişim elde etmek için kullanılan bu teknikler, hedeflenen kimlik avı ve dışarıya açık web sunucularındaki zayıflıklardan yararlanmayı içerir.

İlk Erişim yoluyla kazanılan erişimler, geçerli hesaplar ve harici uzak hizmetlerin kullanımı gibi sürekli erişime izin verebilir veya değişen parolalar nedeniyle sınırlı kullanım olabilir.

İlk Erişim (Initial Access) taktiği kullanılarak yapılan saldırıların **%100'ü ADEO MDR Servisi** tarafından tespit edilebilmektedir.

Kullanıcıların parola belirlerken sosyal ağlarda ve diğer platformlardaki parolalarını kullanmamaları, parolaların değiştirilme aralığının **1 ile 3 ay arasında** olması, özel karakter içermesi ve **minimum 14 karakter** zorunluluğu getirilmesi gerekmektedir.
Hesap yetkilendirme yapılması sırasında gereksiz yetki verilmesinden kaçınılmalıdır. **İşten çıkan personelin hesaplarının kapatılması** önemlidir.

E-posta içindeki **URL incelemesi** (kısaltılmış bağlantıların genişletilmesi dahil), bilinen kötü amaçlı sitelere giden bağlantıların algılanabilmesine yardımcı olabilir. **Sandbox** çözümleri bu bağlantıları algılamak ve kötü amaçlı davranışları belirlemek için otomatik olarak bu sitelere erişim sağlayarak veya bir kullanıcı bağlantıyı ziyaret ederse içeriği beklemek ve yakalamak için kullanılabilir.

Kimlik doğrulama loglarını toplanması ve normal çalışma saatleri dışında olağan dışı/yetkisiz erişimlerin tespit edilmesi gerekmektedir.

Kullanılan uygulama varlık envanterlerinin (web tarayıcıları, bileşenler, eklentiler, ofis ve medya vb.) **düzenli periyotlarda güncelleştirilmesi** önem arz etmektedir.
Tehdit istihbaratı kaynakları tarafından kötü amaçlı olarak sınıflandırılan ağ trafiklerinin **engellenmesi, uyarı oluşturulması sağlanmalıdır.**

17. TAKTİKLER

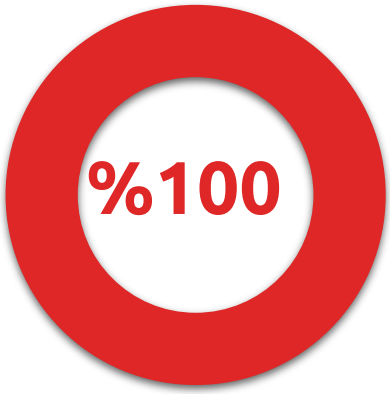
12. YANAL HAREKET (LATERAL MOVEMENT)

Yanal Hareket, saldırganların bir ağdaki uzak sistemlere girmek ve onları kontrol etmek için kullandığı tekniklerden oluşur. Gerçek hedeflerini takip etmek, genellikle hedeflerini bulmak için ağı keşfetmeyi ve ardından ona erişim sağlamayı gerektirir.

Hedeflerine ulaşmak için, genellikle birden fazla sistem ve hesap arasında geçiş yapmayı içerir.

Saldırganlar, yanal hareketi gerçekleştirmek için kendi uzaktan erişim araçlarını kurabilir veya daha gizli olabilecek yerel ağ ve işletim sistemi araçlarıyla meşru kimlik bilgilerini kullanabilir.

Yanal Hareket (Lateral Movement) taktiği kullanılarak yapılan saldırıların **%100'ü ADEO MDR Servisi** tarafından tespit edilebilmektedir.

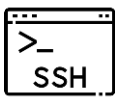


Yanal hareket teknikleri ağ ortamına ve nasıl kullanıldığına bağlı olarak meşru olabilir. **Uzaktan oturum açmadan (RDP)** sonra oluşan erişilen dosyalar ya da gerçekleşen aktiviteler gibi faktörler, bu hareket ile ilgili şüpheli veya kötü amaçlı davranışlara işaret edebilir. Normalde birden çok sisteme nispeten kısa bir süre içinde erişemeyecekleri sistemlerde **oturum açmış kullanıcı hesaplarının izlenmesi önerilir.**

VLAN network ağlarını birbirinden **izole** ederek saldırıların ağda yayılmasına ve veri ihlalerinin önüne geçmektedir.

VPN ile erişilen sistemlerin ya da hizmetlerin sınırlandırılması VPN hesaplarının ele geçmesi durumunda içeride yayılımı minimum düzeyde tutacaktır.

WinRM kullanımı sistem ekipleri tarafından yaygın değilse devre dışı bırakılmalıdır. Eğer yaygın olarak kullanılıyorsa **Windows event logları** yapılandırılmalı ve merkezi olarak **SIEM** üzerinde toplanmalıdır.
Yazılan kurallar ile toplanan bu loglar üzerinden şüpheli erişimler tespit edilmelidir.



SSH kullanımı, ağ ortamına ve nasıl kullanıldığına bağlı olarak meşru olabilir. Uzaktan oturum açmadan sonra oluşan aktiviteler gibi diğer faktörler, **şüpheli veya kötü amaçlı davranışlara** işaret edebilir. Normalde birden çok sisteme nispeten kısa bir süre içinde erişemeyecekleri sistemlerde oturum açmış **kullanıcı hesaplarını izlemek gerekmektedir.**

18. İŞLETİM SİSTEMLERİNE GÖRE KURAL DAĞILIMI

ADEO MDR Servisi olarak **Windows, Linux, MacOS** işletim sistemi ve **türevleri** (*Windows Server, Workstation, Centos, Unix, Debian, Ubuntu tabanlı vb.*) özelinde toplam **4000+** tespit kuralımız mevcuttur.

Geliştirilen tespit kurallarının dağılımı; **Windows işletim sisteminde 3563, Linux 719 ve MacOS ise 695** kural şeklindedir.

Geliştirdiğimiz tespit kuralları **MITRE ATT&CK® Framework**'teki Linux, MacOs, Windows tabanlı tüm işletim sistemleri için oluşturulan **Taktik, Teknik, Prosedürlerin (TTP*)** ortalama **%94'ünü** kapsamaktadır.
Bu sayede tüm müşterilerimize **3 işletim sistemi** ve türevleri için **%96**'nın üzerinde tespit oranıyla destek verebilmekteyiz.

"Tüm müşterilerimize 3 işletim sistemi ve türevleri için %96'nın üzerinde tespit oranıyla destek verebilmekteyiz."

Windows

3500+

LINUX

700+

MacOS

650+

**TTP*
Bir tehdit aktörünün işleyişini açıklamak/tanımlamakta kullanılan Teknik, Taktik ve Prosedürler başlıklarının kısaltmasıdır. TTP'ler belirli bir tehdit aktörünün profilini çıkarmak için kullanılmaktadır.

19. 2023 İLE İLGİLİ ÖNGÖRÜLER

OT ve IoT Sistemler*:

Hem endüstriyel sistemler hem de teknolojinin hız kesmeden gelişmeye devam etmesi, kolaylıkları ile birlikte bazı tehlikeleri de beraberinde getiriyor.

OT (Operasyonel Teknoloji Sistemleri) ve IoT (Nesnelerin İnterneti) siber güvenlik anlamında tehlikeli olabilecek yapıdadırlar.

Örneğin; Florida'da, Team Viewer olarak bilinen uzaktan erişim platformu kullanılarak bir siber saldırı düzenlendi.
Siber saldırganlar, su arıtma sistemine girip, sodyum hidroksit gibi çeşitli bileşenlerin değerlerini kat kat fazlalaştırdılar. Eğer saldırı fark edilmeseydi, insanların zehirlenmelerine yol açılabilirdi.

Siber suçluların motivasyonlarına göre güvenliği konusunda diğer sektörlere göre bir adım geride kalan OT ve IoT sistemler de ileriki zamanlarda saldırıların hedefinde olabilecek gibi görünüyor.

"OT (Operasyonel Teknoloji Sistemleri) ve IoT (Nesnelerin İnterneti) gibi teknolojilerin son zamanlarda siber saldırılardan ciddi şekilde etkilendiği, hatta bu teknolojileri hedef alan özel saldırı tekniklerinin geliştirildiği bilinmektedir."

**Operasyonel Teknolojiler (OT):*
İdari operasyonların aksine endüstriyel operasyonları yönetmek için kullanılan bilgisayar sistemlerini ifade eder. OT, fiziksel cihazların nasıl çalıştığını izleyen ve kontrol eden bir donanım ve yazılım kategorisi olarak da tanımlanabilir. Üretim sistemine ve/veya depolama ve dağıtım sistemlerine sahip işletmeler IT'den tamamen farklı ağ ve cihaz yapısı kullanır. Aynı cihaz anahtar (switch), kablo ve yönlendiriciler kullanıldığı için bu yapının farklılığını anlamak ilk bakışta zordur. PLC'ler, kontrolcüler, sensörler, operatör istasyonlarının hepsinin biraraya gelmesinden oluşan bu yapıya OT (Operasyonel Teknoloji) denilmektedir.

19. 2023 İLE İLGİLİ ÖNGÖRÜLER

Son Kullanıcı Güvenliği:

Siber uzayda her yeni gün, bir güvenlik açığının veya yeni bir saldırı tekniğinin habercisi olabiliyor.
Her ne kadar sıfırıncı gün (Zero-Day) saldırıları gündemi belirleyip siber saldırganların dikkatini çekse de geleneksel yöntemler hala geçerliliğini sürdürüyor.

2022 yılında yeni çıkan ve yaptığı saldırılarla dikkat çekerek adını "Black Basta" olarak duyuran fidye yazılım grubu, ilk erişim (initial access) tekniği olarak hedefli oltalama saldırılarını (spear phishing) kullanarak şirketlere saldırdı.

Oltalama saldırıları ile kurum çalışanlarına ait mail ve parola bilgileri ele geçiriliyor ve hacker forumlarında satışa çıkarılıyor.
Fidye yazılım grupları da saldırmayı hedeflediği kuruma dair bu hassas bilgileri satın alıyor ve saldırı senaryosunu ona göre tasarlıyor.

Bu nedenle günümüzde kurum çalışanlarının siber güvenlik farkındalığını kazanması büyük önem arz ediyor.

Özellikle ;
- Belirli periyotlar ile parolaların yenilenmesi,
- Son kullanıcının bilinçlenmesi adına sosyal mühendislik testlerinin yapılması ve
- İki faktörlü doğrulamanın ihmal edilmemesi siber saldırılara karşı korunma noktasında fayda sağlayacaktır.

**"Oltalama saldırıları ile kurum çalışanlarına ait mail ve parola bilgileri ele geçiriliyor ve hacker forumlarında satışa çıkarılıyor.
Fidye yazılım grupları da saldırmayı hedeflediği kuruma dair bu hassas bilgileri satın alıyor ve saldırı senaryosunu ona göre tasarlıyorlar. "**

ADEO MDR Hizmetlerimiz hakkında detaylı bilgi edinmek ve sorularınızı iletmek için bizimle iletişime geçebilirsiniz.

info@adeo.com.tr

19. 2023 İLE İLGİLİ ÖNGÖRÜLER

Sıfırıncı Gün (Zero-day) Güvenlik Açıkları:

2022'de yeni çıkan ve kendinden söz ettiren bazı sıfırıncı gün (zero-day) zafiyetlerinden raporumuzda bahsettik.

Gündemi takip etmek, özellikle yeni çıkan güvenlik açıklarına karşı üreticilerin yayınladığı yamaları geçmek ve zafiyet barındıran sistemlerdeki anomali faaliyetleri takip etmek çok önem arz ediyor.

E-posta sunucularını etkileyen güvenlik açıklarının yaması yayınlandıktan sonra dahi, çeşitli atlatma (bypass) yöntemlerinin kullanıldığını görüyoruz.

Saldırganlar sunuculara yönelik,
- Yaması yapılmamış, zafiyet barındıran sistemlere erişim sağlarken
- Yaması yapılmış sistemlere ise çeşitli atlatma yöntemleri ile erişmeye çalışacaktır.

E-posta sunucularının yanı sıra, erişim sonrası kalıcılığı sağlamak ve yetki yükseltmek amacı ile kullanılabilecek Active Directory sertifika servislerinde yeni çıkan zafiyetler de kullanılabilir.

2023 yılında e-posta sunucuları ve sertifika servisleri ile ilgili güvenlik açıklarının kullanımının artabileceğini düşünüyoruz.

"2023 yılında e-posta sunucuları ve sertifika servisleri ile ilgili güvenlik açıklarının kullanımının artabileceğini düşünüyoruz."

19. 2023 İLE İLGİLİ ÖNGÖRÜLER

ChatGPT Ne Diyor?

a 2023 yılında olabilecek siber güvenlik saldırıları ne olabilir

Siber güvenlik saldırıları alanında gelecekte ne olacağını tahmin etmek zor bir iştir, ancak bazı olası siber saldırı yöntemleri şunlar olabilir:

1. Ransomware saldırıları: Ransomware, bir bilgisayarı veya veritabanını şifreleyerek, kullanıcıya bir ücret ödemesi talep eden bir saldırı türüdür. Bu tür saldırılar gelecekte daha da yaygın hale gelebilir.
2. İleri teknoloji kullanımı: Yapay zeka ve diğer ileri teknolojiler, siber suçlular tarafından kullanılarak daha sofistike saldırılar yapılabilir.
3. Phishing saldırıları: Phishing, bir kullanıcıyı özel bilgilerini paylaşmaya ikna etmek için yapılan bir saldırı türüdür. Bu tür saldırılar, daha da sofistike hale gelerek, kullanıcıların dikkatsizliğine ve bilgi eksikliğine dayanarak yapılabilir.
4. IoT (Nesnelerin İnterneti) cihazlarını hedef alan saldırılar: Nesnelerin İnterneti (IoT) cihazları, siber suçlular tarafından hedef alınan bir saldırı noktası haline gelebilir. Bu cihazların güvenlik önlemleri yetersiz olabilir ve siber suçlular tarafından kolayca hacklenebilir.

Bu sadece bazı olası siber saldırı yöntemleridir ve gerçekte ne olacağını tahmin etmek çok zor olabilir. Önemli olan, siber güvenlik önlemlerini almayı ve çevrimiçi faaliyetleriniz sırasında dikkatli olmayı sürdürmektir.

“Önemli olan, siber güvenlik önlemlerini almayı ve çevrimiçi faaliyetleriniz sırasında dikkatli olmayı sürdürmektir.”

20. ÖNERİLER #TOP5

1 Olası bir saldırının önüne geçilmesi için kurumların **MSSP** veya **MDR** hizmeti ile **7x24x365** gün izlenmesi gerekmektedir.

2 İkili faktörlü doğrulama **MFA aktif edilmesi**, gereksiz yetki verilmesinden kaçınılması, farkındalığın düşük olduğu yerlerde önleyici önlemlerin alınması önemlidir.

3 Tespit yeteneklerinin artırılması ve bunun için öncellikle görünürlüğün artırılması; ilgili atakları **tespit edecek kuralların** ve **korelasyonların sürekli olarak güncellenmesi** gerekmektedir.

4 Olası siber olaylara karşın hep güncel bir aksiyon planının oluşturulması ve belli periyotlarla **simülasyonların** tekrar edilerek **farkındalığın** ve hazırlıkların **güncel tutulması gerekmektedir.**

5 Varlık envanterlerinin belirli periyotlarda incelenmesi ve **dışarıya açık** olan **servislerin kontrollerinin** sağlanması gerekmektedir.

20. ÖNERİLER

- **IT ve OT** sistemlerinin tamamını kapsayan görünürlük ve sıkılaştırmaların eksiksiz **takip edilmesi önemlidir.**
- Otomatize ürün ve yazılımların, sistemlerin satın alınmasından ziyade **insan temelli servislerin** veya siber güvenlik ekiplerindeki **insanlara yatırımın artırılması** gerekmektedir.
- **Kırmızı Takım (Red Team)** ve **Sızma (Penetrasyon) Testi** aktivitelerinin düzenli periyotlarda uzman ekiplerce gerçekleştirilmesi sağlanmalıdır.
- Saldırıların büyük bir çoğunluğunun yeni çıkan zafiyetlerden kaynaklandığı göz önünde bulundurulmalıdır. Buradan hareketle **"Vulnerability Management" (Zafiyet Yönetimi)** prosedürlerinin sürekli olarak uygulanması ve bunların sıkı bir şekilde takip edilmesi önem arz etmektedir.
- **Oltalama (Phishing)** saldırılarına karşı çalışanlara belirli periyotlarda **farkındalık eğitimlerinin** uygulamalı olarak verilmesi, insan kaynaklı saldırıların önüne geçme noktasında faydalı olmaktadır.
- Siber güvenlik ekiplerinin olgunluk seviyesinin ölçülmesine yönelik Mor Takım **(Purple Team*)** aksiyonlarının, uzman ekiplerce alınması sağlanmalıdır.
- Kurumlarda var olan **ortam** (Active Directory, Firewall, Network Segmentasyon ve varsa diğer güvenlik cihazlarının) ihtiyaca uygun şekilde sıkılaştırılarak, **atak yüzeyi daraltılmalıdır**.

**PURPLE TEAM:*
Mor Takım, Kırmızı Takım ve Mavi Takım'ın birlikte çalışması, iş birliğidir. Kırmızı Takım ve Mavi Takım'ın her ikisinin de beceri ve süreçlerinin geliştirilmesi hedeflenir.

21. ÜRÜN AİLESİNİN YENİ ÜYELERİ

Ürün Ailesinin Yeni Üyesi Crowdstrike

ADEO MDR Servisi'nin ürün ailesine eklenen **Crowdstrike** için kurallar geliştirildi ve geliştirilen **500+ kural** ürüne eklendi.

SOAR ile MDR Daha Güçlü

SOAR (Security Orchestration Automation and Response) teknolojisi MDR hizmetimizin merkezinde yer almaktadır.

Çeşitli araçlar arasında görevleri tek bir platformda yürütmeyi, koordine edebilmeyi, otomatikleştirmeyi sağlayan bu ürün; aynı zamanda var olan insan gücümüzü daha efektif kullanmamıza yarayan bir çözümdür.

SIMSPACE ile Dayanıklılık

ADEO siber güvenlik ekipleri iş ortaklığı kurulan Simspace Eğitim Simülasyon ve tatbikat ortamı üzerinde bilinen ve güncel tehditlere karşı tatbikatlar gerçekleştiriyor. Simspace ile gelişmiş saldırılara karşı evriltilmiş araçlar, süreçler ve ekipler oluşturabilir, optimize edilmiş bir siber dayanıklılık sağlayabilirsiniz.

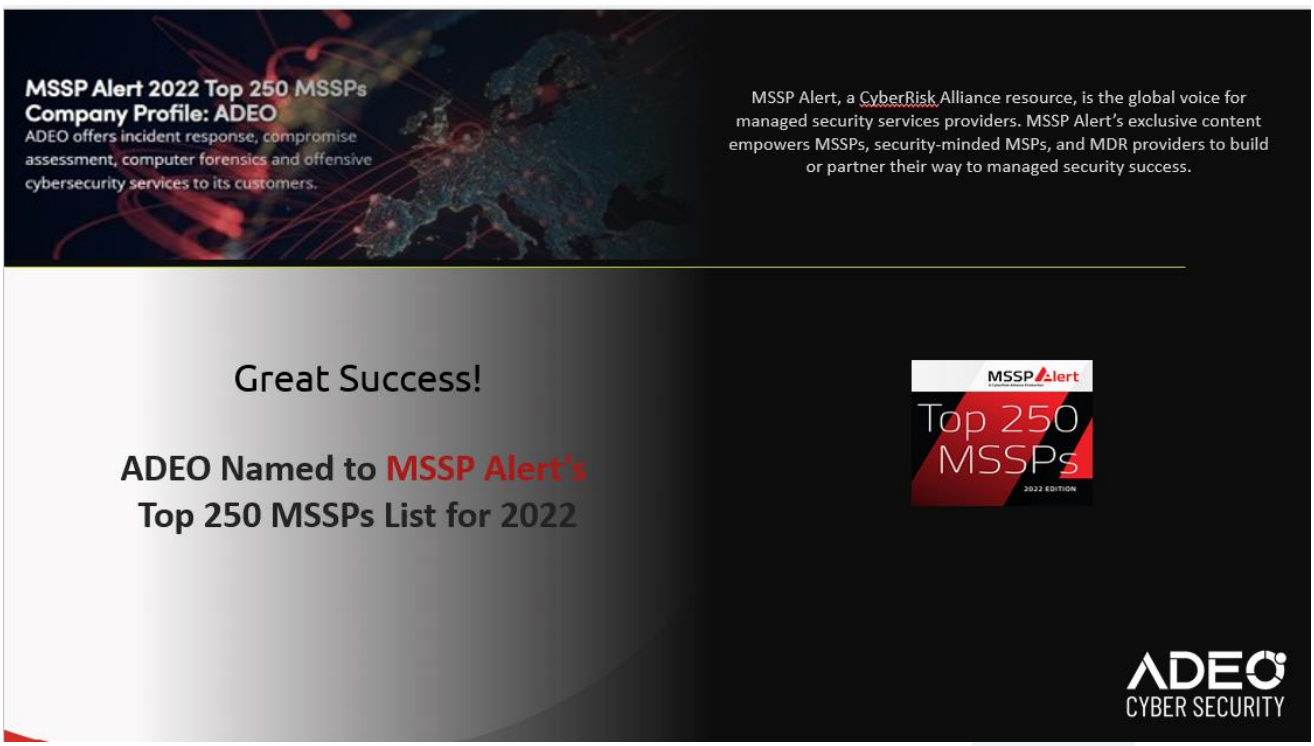
Ürün Ailesinin Yeni Üyesi Cybereason

ADEO MDR Servisi'nin ürün ailesine eklenen Cybereason için kurallar gelistirildi ve gelistirilen **50+** kural ürüne eklendi.

22. 2022'DE ADEO

ADEO Cyber Security "Dünyadaki En İyi 250 MSSP" listesine girdi

**MANAGED SECURITY SERVICE PROVIDERS(MSSP) – YÖNETİLEN GÜVENLİK HİZMETİ SAĞLAYICISI: MSSP, bir kuruluşa uzaktan yazılım/donanım tabanlı bilgi veya ağ güvenliği hizmetleri sağlayan bir tür hizmet sağlayıcısıdır. Bir MSSP, bir veya daha fazla istemciye aynı anda bilgi güvenliği (IS) hizmetleri sağlayarak bir güvenlik altyapısını barındırır, dağıtır ve yönetir.*



22. 2022'DE ADEO

ADEO Cyber Security Microsoft'un liderlik yaptığı ve siber güvenlik sektöründe söz sahibi üreticilerle servis sağlayıcılarını biraraya getiren Microsoft Intelligence Security Association'a (#MISA) dahil oldu.

"MISA üyeliğimiz sayesinde Marketplace'e 2 önemli servisimizi yayınlama şansı edindik. Managed SOC ve MDR servislerimiz Marketplace üzerinden ulaştırabileceğimiz bölgelere verilebilir hale geldi."

22. 2022'DE ADEO

23. İLETİŞİM

MDR Servis Hizmetimiz ile ilgili detaylı bilgi almak için

mdr@adeo.com.tr

üzerinden bizimle iletişime geçebilirsiniz.

İstanbul Merkez

Fetih Mah. Tahralı Sk.
Tahralı Sitesi Kavakyeli Plaza
C Blok D16/17
Ataşehir / İSTANBUL / TÜRKİYE

Telefon: +90 (216) 472 35 35
Fax: +90 (216) 472 35 36

Ankara Şube

Kabil Cad. (Eski 4.Cad)
1335. Sokak No:58 D:9-10
Aşağı Öveçler
Çankaya / ANKARA / TÜRKİYE

Telefon: +90 (312) 482 12 35
Fax: +90 (312) 482 12 36

Email: info@adeo.com.tr

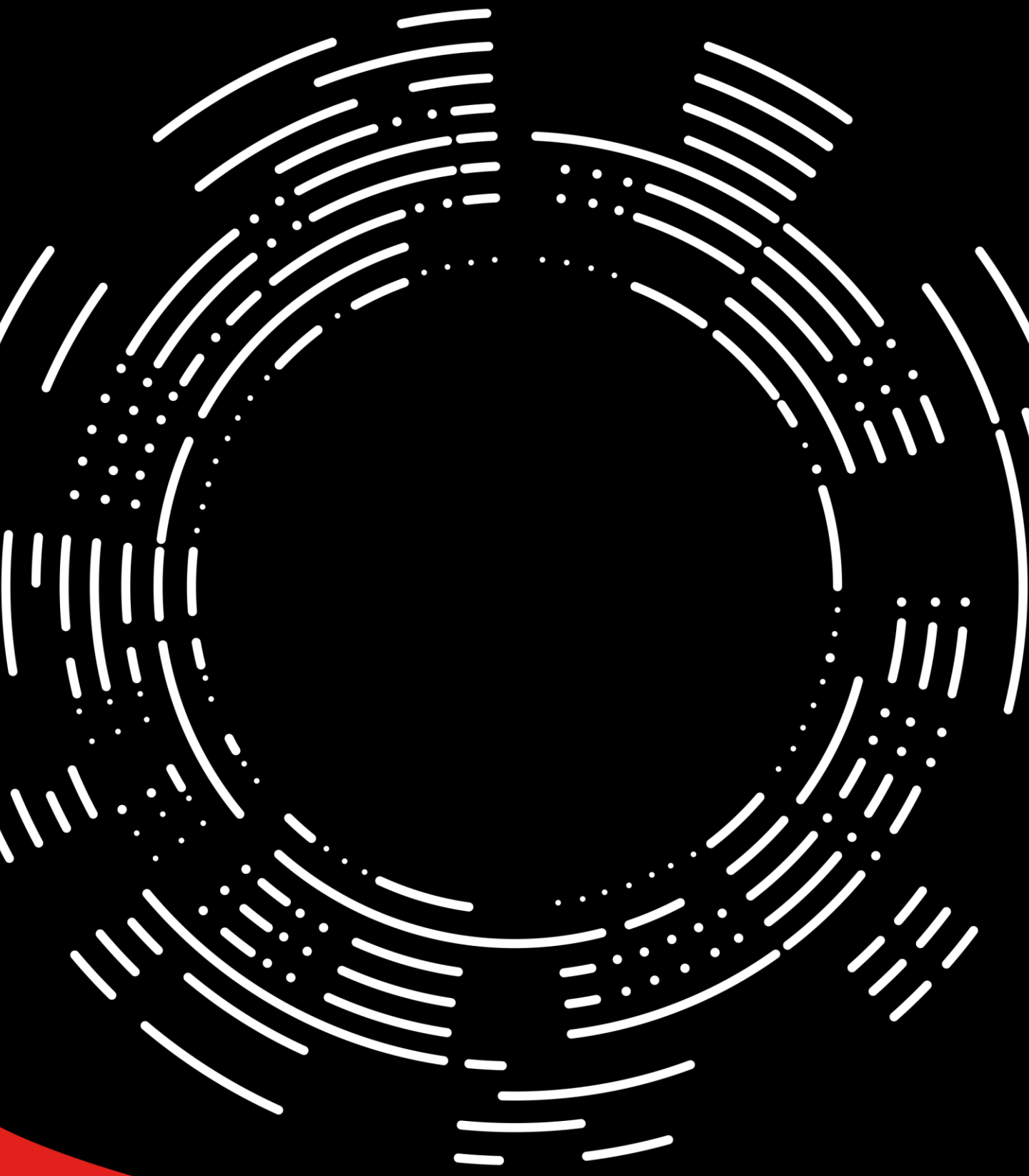
adeo.com.tr
mxdrturkiye.com

/adeosecurity /adeodfir
/adeocomtr

/ADEOcomtr

/ADEO Cyber Security Services

/adeocomtr



www.adeo.com.tr